Detection and Analysis of Malicious Domains Using Machine Learning Techniques

Dr. G. Savitha[1], Mrs. M. Poomani[2], Dr. J. Jebamalar Tamilselvi[3]
[1,2] Assistant Professor, Department of Cyber Security, SRMIST, Ramapuram, Chennai, India
[3] Associate Professor, Department of Cyber Security, SRMIST, Ramapuram, Chennai, India

Abstract

Cyber dangers, particularly bad domains used for phishing, virus distribution, spam, and unauthorized data access, have grown significantly due to the quick expansion of internet usage. Because new harmful websites are constantly appearing, traditional blacklist-based detection techniques are sometimes insufficient. Using domain-related characteristics and classification methods, this study suggests a machine learning-based hazardous domain detection system to efficiently identify dangerous domains. In order to train prediction models that can differentiate between harmful and lawful domains, the system makes use of a dataset that contains information about malicious domains. To increase prediction accuracy and decrease false positives, data preprocessing, feature extraction, and model training are used.By lowering dependency on manually maintained blacklists and facilitating early detection of dangerous domains, the suggested method improves cybersecurity. Results from experiments show that machine learning methods may effectively identify harmful domains with enhanced scalability and detection performance.

1. Introduction

The internet is becoming a necessary tool for commercial operations, financial transactions, communication, and education. Cyber dangers, however, have also increased as a result of the growing reliance on internet services. The presence of bad domains—websites created to spread malware, carry out phishing scams, steal personal data, or carry out illegal activities—is one of the biggest cybersecurity issues.

Blacklisting strategies, which store known harmful websites in a database and block them, are the mainstay of traditional domain security systems. Blacklist techniques are somewhat effective, but they have a number of drawbacks. Real-time database updates are challenging due to the constant creation of new domains by cybercriminals. Because of this, newly created malicious domains frequently get past security measures.

Because machine learning can automatically identify domains and analyze patterns, it has become a potential method for hostile domain detection. Machine learning algorithms can detect suspicious features and determine if a domain is hostile or legitimate by learning from past data. The implementation of a hostile domain identification system utilizing machine learning techniques is the major goal of this project. The suggested approach uses intelligent classification models to efficiently identify risks by analyzing domain-related data from datasets. By offering quicker and more precise detection techniques, the goal is to enhance cybersecurity measures.

Objectives of the Study

- To analyze malicious domain datasets.
- To preprocess and clean domain-related data.
- To implement machine learning techniques for domain classification.

- To improve malicious domain detection accuracy.
- To reduce false-positive detection in cybersecurity systems.

2. Literature Study

Malicious domain identification has been aided by a number of researchers using various techniques.

2.1 Conventional Blacklisting Techniques

Blacklist databases were the primary source of harmful domain blocking for earlier cybersecurity solutions. Security firms kept lists of dangerous websites and blocked users from seeing them. Blacklist techniques are straightforward and efficient, however they are less successful at detecting newly formed malicious domains.

2.2 Detection Based on Machine Learning

Researchers introduced machine learning techniques to improve malicious domain identification. Supervised learning models such as:

- Decision Tree
- Random Forest
- Support Vector Machine (SVM)
- Naive Bayes
- Logistic Regression

have shown effective classification performance.

These methods analyze domain features such as:

- Domain length
- Number of special characters
- IP address behavior
- URL patterns
- DNS records
- Hosting information

Machine learning-based approaches outperform traditional systems because they can generalize patterns and identify unknown malicious domains.

2.3 Deep Learning Approaches

Recent studies have introduced deep learning models such as:

- Artificial Neural Networks (ANN)
- Convolutional Neural Networks (CNN)
- Recurrent Neural Networks (RNN)

These approaches automatically learn hidden domain characteristics and improve classification accuracy. However, deep learning models require larger datasets and higher computational resources.

2.4 Hybrid Detection Techniques

Hybrid systems combine blacklist mechanisms with machine learning models to achieve better performance. These systems utilize historical knowledge while dynamically detecting new malicious domains.

The literature suggests that intelligent detection systems significantly enhance cybersecurity and minimize online threats.

3. Implementation Content

3.1 Dataset Description

The implementation uses a malicious domain dataset containing domain-related information. The dataset includes suspicious and harmful domains collected from cybersecurity sources.

The uploaded dataset (`3_malicious_domains.csv`) is used for training and testing purposes.

The dataset generally contains:

- Domain names
- Malicious labels
- Domain characteristics
- URL-related attributes
- Security classification information

3.2 System Architecture

The proposed malicious domain detection system consists of the following phases:

Phase 1: Data Collection

The malicious domain dataset is collected from cybersecurity repositories and stored in CSV format.

Phase 2: Data Preprocessing

Raw data often contains missing values, duplicate records, and irrelevant features. Preprocessing involves:

- Removing null values
- Eliminating duplicates
- Encoding categorical values
- Feature normalization

Phase 3: Feature Extraction

Important features are extracted from domain names to improve model learning.

Example extracted features:

- Domain Length
- Number of Digits
- Number of Special Characters
- Presence of Suspicious Keywords
- URL Complexity
- Subdomain Count

Phase 4: Model Training

Machine learning algorithms are trained using preprocessed data.

Possible algorithms include:

Random Forest: Random Forest improves prediction accuracy by combining multiple decision trees.

Decision Tree: Decision Tree classifies domains based on feature conditions.

Logistic Regression: This method predicts whether a domain belongs to malicious or legitimate classes.

Support Vector Machine (SVM): SVM separates malicious and safe domains using classification boundaries.

3.3 Implementation Steps

Step 1: Import Dataset

The malicious domain dataset is imported into the system using Python libraries such as:

- Pandas
- NumPy
- Scikit-learn

Step 2: Data Cleaning

Missing values and duplicate entries are removed.

Step 3: Feature Engineering

Text-based domain information is converted into numerical features.

Step 4: Train-Test Split

The dataset is divided into:

- Training Data (80%)
- Testing Data (20%)

Step 5: Model Building

Machine learning models are trained using training data.

Step 6: Performance Evaluation

The trained model is evaluated using performance metrics:

- Accuracy
- Precision
- Recall
- F1 Score
- Confusion Matrix

3.4 Algorithm

Load malicious domain dataset.

1. Clean and preprocess data.
2. Extract meaningful domain features.
3. Train machine learning classification model.
4. Test the model using unseen data.
5. Predict whether domains are malicious or safe.
6. Generate detection reports.

3.5 Advantages of the Proposed System

- Faster detection of malicious domains.
- Reduced dependency on manual blacklists.
- Improved classification accuracy.
- Scalable for large cybersecurity datasets.
- Ability to identify newly emerging threats.

4. Conclusion

Malicious domains continue to be a major cybersecurity challenge due to their involvement in phishing, malware attacks, and unauthorized access activities. Traditional blacklist-based approaches are insufficient for detecting newly emerging threats because attackers continuously generate new malicious domains.

This study proposed a machine learning-based malicious domain detection system capable of identifying suspicious websites through intelligent classification techniques. By analyzing domain characteristics and applying machine learning algorithms, the system improves detection accuracy and enhances cybersecurity protection.

The implementation demonstrates that machine learning methods can effectively classify malicious domains while reducing manual effort and improving response time. Therefore, intelligent domain detection systems are becoming essential tools for modern cybersecurity environments.

5. Future Enhancement

The proposed system can be enhanced in several ways to improve detection capability and efficiency.

1. Deep Learning Integration

Future systems can incorporate deep learning models such as CNN and LSTM to improve feature learning and classification accuracy.

2. Real-Time Detection

The system can be integrated into browsers and firewalls for real-time malicious domain detection.

3. Large-Scale Threat Intelligence

Combining global threat intelligence feeds can improve prediction reliability.

4. Hybrid Security Model

A combination of blacklist, heuristic analysis, and machine learning can improve detection performance.

5. Cloud-Based Deployment

The system can be deployed in cloud environments for scalable cybersecurity monitoring.

6. Explainable AI

Future models can provide explanations for predictions, helping cybersecurity analysts understand why a domain is marked malicious.

References

1. Fan, Z., Wang, Q., Jiao, H., Liu, J., Cui, Z., Liu, S., & Liu, Y. (2022). **PUMD: A PU learning-based malicious domain detection framework**. *Cybersecurity, 5*(19). Springer. DOI: 10.1186/s42400-022-00124-x.
2. Almashhadani, A. O., Kaiiali, M., Carlin, D., &Sezer, S. (2020). **MaldomDetector: A system for detecting algorithmically generated domain names with machine learning**. *Computers & Security, 93*, 101787. DOI: 10.1016/j.cose.2020.101787.
3. Singh, K., Singh, P., & Kumar, K. (2020). **Malicious Domain Detection Using Machine Learning On Domain Name Features, Host-Based Features and Web-Based Features**. *Procedia Computer Science, 171*, 654–661. DOI: 10.1016/j.procs.2020.04.071.
4. Wang, Q., Li, L., Jiang, B., & Lu, Z. (2020). **Malicious Domain Detection Based on K-means and SMOTE**. *IEEE/PMC Cybersecurity Research*. DOI: 10.1007/978-3-030-50420-5_19.
5. Zhao, H., Chang, Z., Wang, W., & Zeng, X. (2019). **Malicious Domain Names Detection Algorithm Based on Lexical Analysis and Feature Quantification**. *IEEE Access, 7*, 128990–128999. DOI: 10.1109/ACCESS.2019.2940554.
6. Vinayakumar, R., Soman, K. P., &Poornachandran, P. (2018). **Detecting malicious domain names using deep learning approaches at scale**. *Journal of Intelligent & Fuzzy Systems, 34*(3), 1355–1367. DOI: 10.3233/JIFS-169431.
7. Wang, Z., Chiong, R., & Fan, Z. (2021). **A fuzzy-weighted approach for malicious web domain identification**. *Journal of Intelligent & Fuzzy Systems, 41*(2), 2551–2559. DOI: 10.3233/JIFS-200943.

8. Wang, Z., Chiong, R., & Fan, Z. (2022). **A fuzzy-based ensemble model for improving malicious web domain identification**. *Expert Systems with Applications, 204*, 117243. DOI: 10.1016/j.eswa.2022.117243.
9. Li, Y., et al. (2020). **DeepDom: Malicious domain detection with scalable and heterogeneous graph convolutional networks**. *Computers & Security, 99*, 102057. DOI: 10.1016/j.cose.2020.102057.
10. Sahoo, D., Liu, C., & Hoi, S. C. H. (2017). **Malicious URL Detection using Machine Learning: A Survey**. *arXiv Preprint*.